STATEMENT

OF

CATHERINE A. ALLEN

CEO, BITS

BEFORE THE

UNITED STATES CONGRESS

HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE,

AND ACCOUNTABILITY

HEARING ON CONTINUITY OF OPERATIONS IN THE FINANCIAL

SERVICES SECTOR POST A MAJOR EVENT

SEPTEMBER 26, 2005

TESTIMONY OF CATHERINE A. ALLEN
CEO, BITS

Introduction

Thank you, Chairman Platts and Representative Towns for the opportunity to submit testimony before the House Committee on Government Reform's Subcommittee of Government Management, Finance, and Accountability on the subject of continuity of operations in the financial services sector post a major event.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS and Roundtable member companies provide fuel for America's economic engine, accounting directly for $40.7 trillion in managed assets, $960 billion in revenue, and 2.3 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues, moving quickly as needs arise. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses. To achieve our mission, BITS also works with government organizations including the U.S. Department of Homeland Security (DHS), U.S. Department of the Treasury, federal financial regulators, the Federal Reserve, technology associations, and major third-party service providers.

As risk managers and leaders in caring for the financial services sector critical infrastructure, the financial services industry has always taken significant steps to prepare for and respond to major events. Events in the past few years—from 9/11 to Hurricanes Katrina and Rita—have escalated our efforts. While I believe our industry overall is better prepared than ever, there are significant risks than can only be addressed by working in partnership with others. My testimony will outline the steps that BITS and others in the financial services industry have taken in recent years and actions the government can take to support our efforts.

The financial services sector is a key part of the nation's critical infrastructure. Customer trust in the security of financial transactions is vital to the stability of the financial services sector and the strength of the nation's economy. Financial institutions weathered Hurricane Katrina, and now Hurricane Rita, well and responded to customer needs quickly. Financial institutions also responded well to the August 2003 power outage and the terrorist attacks on 9/11. We know that our sector is a favorite target of cyber criminals as well as of terrorists, as was made clear on 9/11. Over the past four years, the financial services sector has taken major strides to respond to the risks we face today while preparing to address future threats and vulnerabilities.

The financial services industry has done a great deal to strengthen business continuity planning and to coordinate prior to and during times of crisis. Financial institutions have business continuity plans which they constantly update, refine and test. This is a regulatory requirement and part of the risk management process that financial institutions have embraced based on past experience, robust expertise and changing risks.

As financial institutions identify risks, they worked to mitigate them. BITS has made coordinating financial services industry crisis management efforts a top priority. Senior executives at our member companies have dedicated countless hours to preparing for the worst. We have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sector's Information Sharing and Analysis Center (FS/ISAC), conducted worst case scenario exercises, engaged in partnerships with the telecommunications sector and key software providers, compiled lessons learned from 9/11, the August 2003 blackout and Hurricane Katrina, developed best practices and voluntary guidelines, created a model for regional coalitions, developed liaisons and pilots with the telecommunications industry for diversity and redundancy, and combated new forms of online fraud. Additionally, BITS is now developing best practices in collaboration with the electric power industry to address resiliency and recoverability issues should there be a power failure affecting financial services.

Most recently, in response to Hurricane Katrina, and now Hurricane Rita, BITS has stepped in to assist in coordinating and disseminating critical information. BITS held conference

calls with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS disseminated daily updates to members beginning on September 1, serving as a repository and conduit for timely information. BITS worked closely with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and disseminated key information to our members from regulatory agencies, Treasury and the Department of Homeland Security. Topics included assessment of impacts from the storm, efforts to deliver adequate cash supplies, FEMA's distribution of debit cards to victims of Katrina, talking points for consumer assistance, guidance from regulatory agencies, and important contacts for additional support.

As you know, financial institutions are heavily regulated and actively supervised by state and federal agencies. At the federal level, these include the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Both federal and state level regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. The financial exchanges have also added requirements in these areas. Our industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, BITS and other industry associations have developed and disseminated voluntary guidelines and best practices as part of a coordinated effort to strengthen all critical players in the sector.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications, energy and software industries—must also do their fair share to ensure the soundness of our nation's critical infrastructure.

During the past four years, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (or FSSCC) has been created. I referred to it earlier in the context of the industry's response to Hurricane Katrina. BITS helped to

establish the FSSCC in 2002 and continues to play a major role in its efforts.   Its mission is to coordinate the entire financial sector and act as a focal point for engagement with all the regulators, Treasury, the Department of Homeland Security and the Federal Reserve.   The FSSCC works in concert with the Treasury Department and other government agencies to address critical infrastructure and homeland security issues. The FSSCC is chaired by the financial services sector coordinator, Don Donahue, Chief Operating Officer, Depository Trust and Clearing Corporation, who is also testifying today. The FSSCC fosters and facilitates financial services sector-wide activities and initiatives designed to improve critical infrastructure protection and homeland security, based on a close alliance and cooperation with BITS and among the other FSSCC members to achieve these ends. BITS and other FSSCC members work closely with the Federal Banking Infrastructure Information Committee (FBIIC) under the leadership of the U.S. Department of the Treasury and with the active participation of numerous government agencies responsible for the safety and soundness of the entire financial services sector.

Two other examples of cooperative efforts to assist in preparing for and successfully addressing risks associated with catastrophic events are worth noting. One is our ongoing support for the work of the Department of Homeland Security, and specifically our development, with the Securities Industry Alliance, of a set of considerations for actions to be taken by financial institutions and the sector at each of the DHS levels of homeland security. The second is our work with the U.S. Treasury and a range of organizations in the Chicago area to establish the organization, ChicagoFIRST. ChicagoFIRST was created to foster preparedness and recoverability of financial services in a specific region, and serves as a model for other such organizations throughout the country.

As part of BITS' work to strengthen our nation's critical infrastructure, we have focused on the need for more diverse and resilient telecommunications services. BITS engaged telecommunications companies and government agencies to help mitigate some of these risks. The *BITS Guide to Business Critical Telecommunications Services* is an excellent resource for outlining the financial services industry's requirements from telecommunications service providers, including in times of disruption and crisis. In dealing with Katrina's aftermath,

that earlier work gave us a deeper understanding of the risks we face and the remedies we need to recover.

Attached to my testimony is a comprehensive overview of contributions that BITS made in 2004 and to date in 2005 to address homeland security and critical infrastructure protection concerns (see Appendix A.) Appendix B is a brief description of our activities in response to Hurricane Katrina. Similar activities are underway in response to Hurricane Rita. These efforts support the following key elements of our strategy to protect the financial services sector and its critical infrastructure:

- Improving communications during crises;
- Enhancing the resiliency of telecommunications services;
- Enhancing the reliability of the electrical grid;
- Improving the security of software, hardware and the Internet;
- Addressing new forms of online fraud; and
- Improving oversight of third party providers.

Additional details on the efforts of the entire financial services sector are outlined in a report issued by the FSSCC. See www.fsscc.org for a copy of this report.

Key Elements for Being Prepared

There are numerous lessons we can draw from 9/11, the August 2003 blackout and most recently Hurricanes Katrina and Rita. The most important and obvious is to **be prepared**. An important part of being prepared is looking strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability. Further, it is important that we work with other parties in the private and public sectors to address these issues sufficiently. We understand that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

Diverse and resilient communication channels are essential. Diverse elements—such as cell phones, wireless email devices, landline phones, and the Internet—are required. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained. Closely related to this is the importance of having accurate and timely information about the scope and cause of major events. For example, during the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and enhanced the orderly execution of business continuity processes.

The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation. The cascading impact on the operation of financial services, access to fuel, availability of water, and sources of power for telephone services and Internet communications cannot be overstated.

Recognize the interdependence of all critical infrastructure sectors. Those of greatest concern to us, and relevant to the topic of this Hearing, are the interdependencies between financial services, telecommunications, and energy. We believe the government should take action to enhance the diversity and resiliency of the telecommunications infrastructure and the nation's energy grids.

Recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the nation's critical infrastructures, needs to be explored, including ways of sharing responsibility and liability more equitably. See Appendix C for a list of steps the government can take to strengthen cyber security.

And, as Hurricane Katrina has poignantly made clear, we need to establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur. Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent

On behalf of both BITS and The Financial Services Roundtable, thank you for the opportunity to testify before you today.

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Appendix A

**PROTECTING THE CRITICAL INFRASTRUCTURE:
BITS' ACCOMPLISHMENTS IN 2004 - 2005**

<u>PUBLICATIONS OF BEST PRACTICES AND GUIDELINES</u>

Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy

- The BITS study on "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy" outlines inefficiencies resulting from regulatory overlap within:
  - The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA);
  - The Gramm-Leach-Bliley Act of 1999 (GLBA);
  - The Sarbanes-Oxley Act of 2002 (SOX); and
  - The proposed U.S. Inter-agency Operational Risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) for Regulatory Capital (applying the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also referred to as Basel II), July 2003.
- The study includes specific recommendations for implementation by member institutions to increase efficiencies, and further provides recommendations for regulators to work with the financial services industry to reduce unnecessary burdens and eliminate inconsistent requirements. The study will be available in hard copy in September 2005, and will be jointly distributed by BITS and the Roundtable to key regulators as well as member institutions.

BITS Consumer Confidence Toolkit and Voluntary Guidelines
- BITS has developed a *Consumer Confidence Toolkit: Data Security and Financial Services*. This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS has developed Voluntary Guidelines as recommendations to member institutions for managing information security and consumer confidence issues.

BITS Critical Success Factors for Security Awareness & Training Programs
- Under the auspices of the BITS Security and Risk Assessment Program, BITS developed a description of critical factors for establishing and maintaining a comprehensive security awareness and training program for financial institution personnel. Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice.

BITS Key Considerations for Global Background Screening Practices
- BITS released the *BITS Key Considerations for Global Background Screening Practices* on June 29, 2005. This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The paper is divided into three sections:
  - Overview of the financial industry's legal and regulatory requirements;
  - Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
  - Information to validate identity and background, listed by country.
- Each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements. The paper is available on the BITS website at www.bitsinfo.org on the publications page.

Key Contractual Considerations for Developing an Exit Strategy
- Published in May, 2005, the *BITS Key Contractual Considerations for Developing an Exit Strategy* provides detailed suggestions for contracts with third party service providers, many of which provide security-related services and affect critical infrastructures.

Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments
- Loan fraud is a fast-growing problem. This Members' Only guide helps financial institutions catch loan frauds as they happen and recover from related losses. Members interested in obtaining a copy may access it via the BITS site, www.bitsinfo.org, in the Members' Only area.

BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings
- In January 2005, BITS published the *BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings.* This Members' Only guide assists financial institutions in understanding technology to verify and authenticate online users and determine the level of risk users pose to the institution. This document was created to help financial institution fraud managers as they explore these technologies and identify those that may be appropriate for their needs. This paper focuses on technology solutions for:
  - Verification. These products screen data elements provided by a client to ensure the elements (Social Security numbers, addresses, etc.) are real.
  - Authentication. Once the data elements are verified, authentication products ensure the credentials given belong to the person providing them.

–   Financial experience information. Having verified the data elements and authenticated the customer, financial experience information determines the level of risk assumed by accepting the potential customer.

BITS Guide to Business-Critical Telecommunications Services

*   On November 15, 2004, BITS released the *BITS Guide to Business-Critical Telecommunications Services*. The *BITS Guide* highlights questions business continuity planners and other risk managers should ask themselves as well as an overview of key points to consider in risk assessment, due diligence, contracting, testing and monitoring processes of their telecommunications services.

Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions

*   The U.S. Department of the Treasury publicly released the handbook, "Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions" on December 7, 2004. This handbook is the result of a collaborative effort, funded by Treasury and co-authored by BITS, The Boston Consulting Group and ChicagoFIRST. The handbook offers "lessons learned" and clear recommendations for replicating the success of the ChicagoFIRST model in other regions. Louis F. Rosenthal, Executive Vice President, LaSalle Bank Corporation, and Ro Kumar, First Vice President of The Options Clearing Corporation are to be commended for their leadership and vision as founding co-chairs of the coalition. Teresa Lindsey, BITS Chief of Staff, was instrumental in facilitating the development of ChicagoFIRST and in distilling the "lessons learned."

BITS Kalculator: Key Risk Management Tool for Information Security Operational Risks

*   The *Kalculator* starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the *Kalculator*, financial institutions score their information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. Companies can use the results to boost their ability to assess and mitigate risks. The *Kalculator* is unique in that it brings together information security risk categories from international security standards and emerging operational risk regulatory requirements into one tool that can be easily customized.

Developing a KRI Program: Guidance for the Operational Risk Manager

*   The document, *Developing a KRI Program: Guidance for the Operational Risk Manager*, helps operational risk managers establish and maintain strong KRI programs in an environment of increased operational risk regulation.

Best Practices in Patch Management for the IT Practitioner

*   *BITS Best Practices in Patch Management* provides critical recommendations for an enterprise approach to managing patches. Divided into 10 sections reflecting the components of effective patch management processes, the document provides

considerations for defining roles, responsibilities and tools; developing and maintaining an inventory of IT infrastructure; developing a "standard build"; and verifying patch installation. While created for financial institutions, these recommendations may be applied to other industries.

BITS IT Service Providers Expectations Matrix

- The BITS *IT Service Provider Expectations Matrix* provides financial institutions, service providers, and audit and assessment organizations with comprehensive and consistent expectations to reduce risk. Presented in an Excel spreadsheet, it outlines financial institution expectations for the security of information and personnel, as well as policies and processes for ensuring physical security. The expectations address critical disaster recovery/business continuity issues necessary to ensure products and services are supported by and coordinated with service providers.

Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act

- This paper provides informed analysis of the risks and benefits associated with implementation of the Check 21 Act. Strategies for mitigating risks are included as well as a matrix that describes Check 21-related risks and mitigants from the standpoint of three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank.

COMMENT LETTERS

Comment Letter on FDIC Study, "Putting an End to Account-Highjacking Identity Theft"

- BITS, The Financial Services Roundtable and the Identity Theft Assistance Corporation jointly submitted a comment letter, raising concerns about the proposed approach to remedies for fraud-related security risks. The study did not adequately take into account the fact that financial institutions are applying a risk-based approach for evaluating the risks, deploying controls and offering convenient solutions to their customers and recommended solutions that are complex, unwieldy, and, in some instances, will not provide the intended remedy.

Comment Letter on Department of Homeland Security (DHS) Interim Rule on Procedures for Handling Critical Infrastructure Information

- BITS and The Financial Services Roundtable submitted a comment letter to DHS on a rule to establish "uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security." The letter outlines concerns about the scope and implementation of the procedures. It states that DHS must implement robust controls to adequately protect employees and customers of financial institutions.

"The Department of Homeland Security Cybersecurity Enhancement Act of 2005" to House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

- Catherine A. Allen, BITS CEO, testified in April, 2005 on the importance of elevating the position of Cybersecurity Director at the Department of Homeland Security to an Assistant Secretary level. Her testimony included a description of the current cybersecurity landscape, and what BITS and the industry are doing to address threats. The testimony also included the BITS recommendations to the government to strengthen cybersecurity, referred to in detail and presented as the acronym PREPARE©.

"Critical Infrastructure Protection" to House Financial Services Committee

- Wilton Dolloff, executive vice president for operations and technology at Huntington Bancshares and BITS Executive Committee member, testified in September on behalf of BITS and The Financial Services Roundtable before the House Financial Services Committee. The full Committee hearing was on efforts to strengthen the nation's critical infrastructure. Dolloff emphasized that all critical infrastructure sectors need to participate in ensuring the soundness of the nation's critical infrastructure.

"Information Security—Vulnerability Management Strategies and Technology" to House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census"

- Louis Rosenthal, LaSalle Bank Corporation, testified before Congress on June 2, 2004 on how the financial services industry is working to improve software security. The hearing, titled "Information Security – Vulnerability Management Strategies and Technology," took place before the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Mr. Rosenthal testified on behalf of BITS and the Roundtable. He shared BITS' data on the enormous cost of addressing software vulnerabilities, including managing patches (approaching $1 billion annual cost to the industry). Mr. Rosenthal stressed that BITS is working to improve the quality of the software financial institutions use through a number of projects. He emphasized, however, that the industry must have the support of its vendor partners and government in order to be successful. His recommendations were based on those of the April BITS/FSR software security policy statement.

SUMMITS, FORUMS AND CONFERENCES

Critical Infrastructure Protection

- John Carlson represented BITS at a July 11, 2005 invitational meeting convened by Bob Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security. The purpose of the meeting was for DHS to get input and recommendations from association leaders who are active in cyber security issues.

- On June 17, 2005 Dartmouth's Institute for Information Infrastructure Protection (I3P) hosted a forum on "Financial Services Challenges in the Cyber World" at New York University in New York City. BITS participated in a panel discussion along with representatives from BITS member companies and key federal government agencies. Approximately 25 government and academic leaders involved in research on cyber security and critical infrastructure issues participated in the meeting.

A Strategic Look at Authentication
- On March 8, 2005, BITS hosted a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum focused on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

BITS Regulatory Forum
- The BITS Regulatory Forum was held on April 26, 2005 and established a dialogue among regulators and financial services firms on the impact of regulatory requirements and supervisory processes. Many of those requirements relate to critical infrastructure protection and security issues. Participants reviewed steps to be taken by all parties to increase efficiency in the regulatory and supervisory process. Senior level regulators and BITS members took part in this session, the first step in an iterative, cross-sector process. The Forum was the first public release of the study, developed on BITS' behalf by KPMG, "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy."

SRA Protecting the Core Forum: Strategies for Securing Your Technology Infrastructure
- On October 6, 2004 BITS held a Forum, "Protecting the Core: Strategies for Securing Your Technology Infrastructure." The invitation-only event allowed member companies and invited vendors to explore how significant risks and costs resulting from insecure devices, untrusted systems, and new threats and vulnerabilities impact core operations. During the Forum, executives from the financial services industry, federal government and top technology companies shared their perspectives as speakers and panelists. Speakers included Burt Kaliski, RSA Security; Scott Charney, Microsoft; Alan Paller, SANS Institute; Ido Dubrawsky, Cisco Systems; Howard Schmidt, eBay; and Edward Amoroso, AT&T. The Forum focused on sharing best practices and identifying solutions.

BITS Critical Infrastructure Forum: Strengthening Resiliency of the Telecommunications and Energy Sectors
- The BITS Critical Infrastructure Forum, "Strengthening Resiliency of the Telecommunications and Energy Sectors," was held June 9, 2004 in Washington, DC. More than 100 participants from the financial services, telecommunications, energy, and chemical sectors attended. Don Monks, The Bank of New York Company, Inc., keynoted, discussing lessons learned from 9/11. Other speakers included Fran Dramis, CIO of BellSouth, Steve Malphrus, Staff Director of the Federal Reserve Board of

Governors, Wayne Abernathy, Treasury Assistant Secretary for Financial Institutions, and Jim Caverly, Director of the Infrastructure Coordination Division in the Information Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security.

BITS and The Financial Services Roundtable Software Security CEO Summit

- The BITS and Financial Services Roundtable Software Security CEO Summit was held February 4, 2004 in Arlington, Va. This invitation-only event allowed member CEOs and CIOs to come together with the CEOs and CIOs of the chemical, telecommunications, and electric industries to discuss how risks and costs resulting from software vulnerabilities are affecting their institutions, and to develop solutions. Senior executives from the financial services industry, federal government and top software companies shared their perspectives as speakers and panelists. Taken from the industry's perspective as leading purchasers of software products, the Summit focused on identifying solutions for improving software security. Eighty participants representing senior leadership from the financial services industry, software providers, other business sectors and government discussed issues and costs related to software security and patch management—and a plan for action to address them. As follow-up to the Summit, BITS Chairman Jim Rohr, The PNC Financial Services Group, distributed a *Software Security Toolkit* to all BITS members and Summit participants.

BITS/American Banker Financial Services Outsourcing Conference

- The Fourth Annual BITS/American Banker Outsourcing Conference, will take place on November 7-8, 2005 at the Renaissance in Washington D.C. This year's agenda will follow four key themes:
    - Governance: Best practices of financial institutions and service providers.
    - Compliance: Strategies for negotiating the current landscape and requirements for privacy and security.
    - Risk Management: Strategies, controls and processes to coordinate risk management across the enterprise.
    - Change: Practical guidance for managing today's dynamic relationships.

- The Third Annual BITS/American Banker Outsourcing Conference, "Managing Risk in a Global Economy," was held on November 8 and 9, 2004 in Washington, DC. Over 150 participants representing financial institutions, regulators and service providers attended. The conference focused on four key themes:
    - Legislative and Regulatory: Strategies for negotiating the current landscape and requirements
    - Privacy and Security: Establishing and maintaining controls and requirements
    - Governance: Creating enterprise-wide accountability and strategies to effectively and efficiently manage your relationships
    - Risks and Opportunities: Identifying best (and worst) practices

Fighting Identity Theft: Outsmarting the Crooks (Joint with U.S. Treasury)
- The Treasury and BITS jointly held a Forum for consumers, "Fighting Identity Theft: Outsmarting the Crooks" on May 26, 2004 in Kansas City, Mo. The event was co-hosted by Wayne Abernathy, Treasury Assistant Secretary for Financial Institutions, and Catherine Allen, BITS CEO. Catherine outlined the financial services industry's efforts to prevent identity theft and assist victims, including the industry's Identity Theft Assistance Center, co-founded by BITS, The Financial Services Roundtable, and 50 founding member financial institutions. She also moderated a panel on innovative technologies the industry is developing to fight identity theft. Abernathy spoke about the tools available to consumers through the Fair and Accurate Credit Transactions (FACT) Act and moderated a panel discussion of the ways financial institutions are helping consumers to fight identity theft.

POLICY DEVELOPMENT

NOTE: BITS serves as a source of fact-based information in the development of policy positions. Following are recent examples, resulting either in a formal position from both BITS and The Financial Services Roundtable, or indirectly, through participation in national-level councils, working groups and task forces. Other examples of BITS' role in policy development are listed above in the categories of Comment Letters and Testimony.
- Joint BITS and Financial Services Roundtable Policy on Authentication Mandates
- Joint BITS and Financial Services Roundtable Policy on Spyware
- Joint BITS and Financial Services Roundtable Policy on Software Security
- Joint BITS and Financial Services Roundtable Policy on Internet Fraud and Phishing
- Support for President's National Infrastructure Advisory Council (NIAC)
- Participation in National Security Telecommunications Advisory Council (NSTAC) Financial Services Task Report
- Participation in Network Reliability and Interoperability Council (NRIC) VII
- Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG)
- Participation in the National Cyber Security Partnership

PILOTS AND PROJECTS

BITS Phishing Prevention and Investigation Network
- BITS is responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS created a Phishing Prevention and Investigation Network. The BITS Phishing Prevention and Investigation Network has three primary purposes. First, the Network helps financial institutions shut down online scams. Second, it helps increase arrests and investigations of scam perpetrators by providing trend data. Law enforcement agencies can use the data to build cases and stop scamming operations. Finally, the BITS

Network facilitates communication among fraud specialists at financial institutions, law enforcement agencies and service providers, resulting in a "united front" for combating online scams. Financial institutions can also use the BITS Network to share information about online scams. Through its searchable database, fraud professionals at BITS member institutions learn from other institutions' phishing incidents and responses. The database provides quick access to contacts at law enforcement agencies, foreign governmental agencies, and ISP administrators. Founded under the auspices of the BITS EScams Subcommittee of the BITS Internet Fraud Working Group, the Network is hosted by the Financial Services Information Sharing and Analysis Center (FS/ISAC). Resources to develop the Network were contributed by Microsoft Corporation and RDA Corporation.

ChicagoFIRST

- With the encouragement of the US Treasury and support from BITS, Chicago's premier financial services institutions formed ChicagoFIRST in July 2003 as an industry coalition that addresses homeland security issues requiring a common response by Chicago's financial services sector. This initiative was prompted by a consensus that existing activities at the regional level did not adequately address the critical infrastructure protection concerns of Chicago's financial institutions. The mission of ChicagoFIRST is:
  - To increase the resilience of the Chicago financial services industry in the event of a regional disaster in collaboration with the city, state and federal agencies, including to:
    - protect the lives of the thousands of people that work in the industry;
    - protect the financial assets that have been entrusted for safe keeping and investment;
    - work directly with city and state authorities on emergency coordination and evacuation; and
    - implement the primary objectives in a rapid manner.

The "lessons learned" from ChicagoFIRST, as reported above and funded by the U.S. Treasury, were published in December 2004, with the hope that additional coalitions will successfully establish similar organizations to strengthen critical infrastructures at a regional level. The Treasury supports the concept of regional coalitions of financial services firms and will work with interested parties to facilitate their formation. For more information, please contact the Office of Critical Infrastructure Protection and Compliance Policy at (202) 622-2602.

Facilitation of Alliance for Telecommunications Industry Solutions (ATIS) Diversity Assurance Pilots

- BITS is working closely with the Alliance for Telecommunications Industry Solutions (ATIS) CIO Council on diversity-assurance pilots. (ATIS is a US-based body that works to develop and promote technical and operations standards for the communications and related IT industry worldwide.) The primary goals of the pilots are to:
  - Assess the basic requirements for an effective diversity-assurance service that meets customer needs and regulatory requirements;
  - Determine the scalability and viability of a manual process patterned after the service provided to the FAA;
  - Identify the best and most effective practices for assuring diversity in a manual mode; and define the requirements for a possible mechanized process.

Identity Theft Assistance Center (ITAC)

- The Identity Theft Assistance Center (ITAC) was initiated as a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and by enabling law enforcement to identify and prosecute perpetrators of this crime. The ITAC is now officially up and running as the pilot was a success. As of August 2005, more than 2500 victims of identity theft had received assistance from the ITAC. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. The ITAC's services are free-of-charge to customers and made available based on referrals to the ITAC by one of the ITAC's Members. For additional information, go to www.identitytheftassistance.org.

BITS Product Certification Program (BPCP)

- The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency and National Institutes of Technology and Standards. DHS has expressed support for broad-based, not sector specific, certification programs. Moreover, DHS wants "buy in" from the broader user community. Consequently, BITS has been in discussions with The Business Roundtable, NIST, and the Cyber Security Industry Alliance (CSIA) to develop a joint proposal.

Joint Work Plans with Major Software Providers

- BITS' efforts to improve the quality of software security have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them. To facilitate achievement of these objectives, BITS has implemented a joint work plan with one major software provider and is developing joint work plans with others.

SURVEYS AND RESEARCH

Cybersecurity R&D Priorities.

- The results of a 2005 BITS survey on cybersecurity research and development are being used to advise the federal government (Congress, Treasury, the Department of Homeland Security) on its R&D priorities. The BITS survey coincides with the

publication of a Cyber Security Industry Alliance (CSIA) paper urging the federal government to play a larger role in coordinating cyber security R&D funding. The CSIA paper notes that while the private sector contributes the majority of funds for R&D on cyber security, most of this money is for short-term solutions to existing problems. The CSIA and BITS are recommending the federal government organize long-term cyber security research to address problems before they emerge.

FOR ADDITIONAL INFORMATION, CONTACT:
Catherine A. Allen, CEO
John Carlson, Senior Director
BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004
(202) 289-4322
cathy@fsround.org
john@fsround.org
www.bitsinfo.org

ABOUT BITS
BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

<center>**Appendix B**</center>

<center>**BITS Hurricane Katrina Response (as of September 12, 2005)**</center>

Provided Daily Updates to Members. BITS disseminated daily updates beginning on September 1 to the BITS Advisory Council, BITS Crisis Management Coordination Key Contacts and Working Group, BITS Fraud Reduction Steering Committee, and Financial Services Roundtable staff. Daily updates included key information from regulatory agencies, Treasury and the Department of Homeland Security on impact assessments on infrastructure (e.g., telecom, power), efforts to deliver adequate cash supplies, distribution of debit cards by FEMA and the Red Cross to victims of Katrina, talking points for consumer assistance, and important contacts for additional support and to request mobile ATMs and satellite phones.

Hosted BITS Working Group Calls and Assisted Members. BITS held several conference calls (September 2 and 6) with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS also participated in other calls by SIA and DHS to gather and serve as a repository of financial sector information.

- BITS Fraud Reduction Steering Committee (FRSC) calls focused on potential fraud and risk mitigation strategies. The FRSC asked BITS to act as a repository of information to help identify and socialize fraud trends and events as they happen.
- BITS acted as primary point of contact for Roundtable members' questions and requests for more information from DHS, Treasury and Regulators. For example, BITS assisted in finding information on where FEMA is transporting large numbers of Katrina evacuees (so that member can be better prepared) and information on which parts of the storm's disaster areas residents have been ordered to evacuate.

Coordinated with FSSCC. BITS staff maintained daily contact with Don Donahue, sector coordinator for the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). BITS provided input to a press release issued by the FSSCC on September 6. The press release outlined the sector's efforts to respond to the crisis. It provided a brief overview of the progress of the financial services sector response to the needs of customers and victims affected by Hurricane Katrina, including:

- Customers of financial institutions located in the affected areas can remain confident that our members and the sector are working constantly to ensure the continued security of their financial assets.
- Deposit insurance (thru the FDIC and NCUA) is in full force.
- Financial institutions activated business continuity plans and some institutions were operating out of their back-up sites.
- National systems for processing of payments and security settlement transactions were unaffected by the hurricane and were operating normally.
- ACH credits for Social Security payments to residents in the affected areas were generally received by the processing financial institutions.

Assisted Roundtable and Members. BITS joined The Financial Services Roundtable's Government Affairs staff in a briefing for the House Financial Services Committee on Wednesday, September 7. BITS prepared a written statement on efforts, however, the committee adjourned before BITS and other associations could speak.   BITS assisted Roundtable colleagues in collecting and disseminating information regarding Roundtable members' charitable donations and relief efforts.

BITS

FINANCIAL SERVICES
ROUNDTABLE

Appendix C

PREPARE

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology. These elements form the acronym, PREPARE©.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.
- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a

limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

- Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.
- Train government employees on proper cyber security measures.
- Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.

- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:
- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:
- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:
- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

For additional information, contact:
Catherine A. Allen, CEO, BITS
Or
John Carlson, Senior Director, BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004
(202) 289-4322
cathy@fsround.org
john@fsround.org
wwwbitsinfo.org